# Kraków, dnia 29.09.2020 r.

## WK-I.2370.15.11.2020

**STRONA INTERNETOWA**

**Dotyczy:** Postępowania przetargowego pn.: „Rozbudowa środowiska sieci LAN i WLAN oraz dostawa i implementacja rozszerzenia zintegrowanego systemu łączności wraz z dostosowaniem automatyki dla Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie.”

(nr sprawy WK-I.2370.15.2020).

Szkoła Aspirantów Państwowej Straży Pożarnej w Krakowie os. Zgody 18, w odpowiedzi na zapytanie firmy, podaje wyjaśnienie dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ).

**Pytanie 1:**

*W ramach Specyfikacji Istotnych Warunków Zamówienia, Zamawiający w załączniku nr 1.1 - Opis przedmiotu zamówienia dla zadania nr 1 w punkcie 4.1.1 Zapora sieciowa UTM USG6310S. Firewall Huawei USG6310S został wycofany ze sprzedaży. Czy w związku z powyższym zaakceptują Państwo możliwość zaoferowania modelu z nowej serii Huawei USG6500E, spełniającego wymagania z wyjątkiem funkcjonalności:*

* *obsługi modemów zewnętrznych USB (3G, 4G LTE),*
* *uwierzytelniania użytkowników przez SecureID,*
* *filtru Antyspam,*
* *systemu umożliwiającego tworzenia map sieci wewnętrznych opartych o szczegółowe informacje MAC i system operacyjny,*
* *tunelowania protokołem PPTP?*

**Odpowiedź 1:**

Zamawiający zmienia zapisy SIWZ załącznik nr 1.1. „Opis przedmiotu zamówienia dla zadania nr 1”, pkt 4.1.1. na:

„Zapora sieciowa UTM USG6500E -**2 szt.**

Minimalne wymaganie techniczne dla pojedynczego urządzenia typu firewall. W ramach

postępowania należy dostarczyć 2 zestawy:

Przedmiot zamówienia objęty jest stawką podatku od towarów i usług w wysokości: 0% - na podstawie Ustawy o podatku od towarów i usług, z dnia 11.03.2004 r., art. 83 ust. 1 pkt. 26 (Dz.U. 2020 poz. 106).

* Wymagania sprzętowe:
* Wydajność firewalla dla pakietów o wielkości 1518/512/64B – 1.2/1.2/1.2 Gbps
* Wydajność modułu IPS – 600Mbps
* Ilość jednoczesnych połączeń – 300 000
* Ilość nowych połączeń na sekundę – 20 000
* Wydajność VPN IPSec – 1 Gbps
* Ilość jednoczesnych tuneli IPsec – 1 000
* Możliwość utworzenia 1000 polityk bezpieczeństwa
* Ilość tuneli SSL VPN – min. 100. Jeżeli funkcjonalność SSL VPN wymaga licencji to należy dostarczyć wraz z urządzeniem licencję na obsługę minimum 100 równoległych sesji SSL VPN
* Zasilanie AC 230V
* Możliwość instalacji w szafie RACK. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria do montażu w szafie RACK
* Dedykowany system operacyjny firewalla opracowany przez producenta urządzenia
* Urządzenie musi posiadać następującą ilość interfejsów:
* Minimum 2 porty 1G SFP. Obsługa modułów optycznych 1G-SX, 1G-LX
* Minimum 10 portów 10/100/1000Base-T
* Port konsoli szeregowej
* Minimum jeden port USB
* Mechanizmy ochrony sieci IP w wersji IPv6
* Obsługa protokołów routingu dla IPv6: BGP4+, IS-ISv6, OSPFv3 oraz RIPng
* Obsługa protokołów routingu dla IPv4: RIP, OSPF, BGP, IS-IS
* Możliwość uruchomienia funkcjonalności IPS, AV, URL filtering oraz AS. Wraz z urządzeniem ma być dostarczona subskrypcja na aktualizację wszystkich funkcjonalności UTM minimum na 2 lat
* Możliwość uruchomienia przynajmniej 10 wirtualnych firewalli. Jeśli jest wymagana licencja urządzenie powinno być dostarczone z licencją na 10 wirtualnych firewalli
* Możliwość uruchomienia funkcjonalności NAT w tym translacja adresu IP źródłowego, translacja adresu IP przeznaczenia, PAT, translacja statyczna i translacje puli adresów IP
* Wsparcie dla funkcjonalności ASPF
* Możliwość konfiguracji kontroli dostępu na podstawie adresów źródłowych i docelowych, portów, typu protokołu, czasu, TOS, użytkownika oraz aplikacji rozpoznawalnej przez analizę warstwy siódmej
* Integracja z wewnętrzną i zewnętrzna bazą użytkowników
* Ochrona przed atakami typu SYN flood, ICMP Flood, IP spoofing, UDP Flood, Land, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, skanowanie adresów oraz portów, IP Option control, IP fragment, large ICMP packet, ICMP redirect packet, ICMP unreachable
* Ograniczanie pasma dla ruchu P2P poprzez tworzenie odpowiednich polityk. Możliwość tworzenia różnych polityk ograniczania pasma dla ruchu przychodzącego i ruchu wychodzącego
* Wykrywanie i kontrolowanie ruch P2P poprzez identyfikację aplikacji typu P2P
* Wsparcie dla funkcjonalności Policy Based Routing (PBR)
* Wsparcie dla protokołów tunelowania: SSL VPN, IPSec VPN, L2TP VPN, GRE VPN, L2TP over IPSec oraz GRE over IPSec, DSVPN
* Wsparcie dla funkcjonalności IPS. Wykrywanie anomalii w różnych protokołach, w tym w: HTTP, SMTP, FTP, POP3, IMAP4, NETBIOS, SMB, MS\_SQL, Telnet, IRC oraz DNS
* Wykrywanie rodzaju protokołu poprzez zawartość danych: HTTP, SMTP, FTP, POP3, IMAP4, MSRPC, NETBIOS, SMB, MSSQL, Telnet, IRC, TFTP, eMule oraz eDonkey
* Grupowanie sygnatur IPS na kategorie
* Możliwość definiowania sygnatur IPS przez użytkownika
* Automatyczna aktualizacja bazy sygnatur IPS poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji
* Możliwość powiązania polityk IPS z regułami ACL i przypisania polityk IPS do strefy
* Możliwość włączania i wyłączania jednej lub wszystkich reguł IPS w polityce oraz konfiguracji rodzaju reakcji na zdarzenie
* Możliwość włączenia i wyłączenia funkcji IPS globalnie dla całego urządzenia
* Możliwe rodzaje reakcji na zdarzenie IPS: logowanie i blokowanie pakietów
* Wysyłanie logów z modułu IPS do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich źródeł i przeznaczenia
* W zależności od ustawień przesłanie danych dalej lub blokada w przypadku przeciążenia modułu IPS
* Wsparcie dla funkcjonalności antywirus (AV). Skanowaniu różnych protokołów w celu wykrycia wirusów. Wsparcie dla wykrywania wirusów w plikach przesyłanych przez HTTP, SMTP, POP3,IMAP,NFS,SMB oraz FTP
* Dekompresja wielokrotnie skompresowanych plików
* Możliwość automatycznej aktualizacji bazy wirusów poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji. Możliwość wylistowania wirusów zawartych w bazie AV
* Możliwość usunięcia wirusa, wyświetlenie strony alarmującej, oznaczanie wiadomości mailowej oraz logowanie
* Możliwość powiązania polityk AC z regułami ACL i przypisania polityk AV do strefy
* Możliwość włączenia i wyłączenia funkcji AV globalnie dla całego urządzenia
* Możliwość wysyłania logów z modułu AV do serwera syslog. Możliwość wygenerowania raportów z modułu AV
* Możliwość przesłania ruchu danych dalej lub ich blokada w przypadku przeciążenia modułu AV
* Wsparcie dla funkcjonalności URL filtering.

Obsługa dopasowywania wpisów w whitelist oraz blacklist w oparciu o prefiks, sufiks słowa kluczowego. Blacklist i whitelist mają wyższy priorytet niż kategoria URL. Whitelist ma wyższy priorytet niż blacklist.

* Obsługa kategorii URL tworzonych przez użytkownika. Kategorie stworzone przez użytkownika mają wyższy priorytet od predefiniowanych kategorii
* Możliwość otrzymania kategorii URL z serwera kategorii dostępnego w sieci Internet. Reakcja podejmowana jest na podstawie skonfigurowanej polityki i przypisanej akcji do konkretnej grupy URL
* Możliwe reakcje modułu URL filtering – „zablokuj” lub „zezwól”;. Możliwość wyświetlenia częściowo spersonalizowanej strony informującej o zablokowaniu dostępu.
* Polityka filtrowania URL może być oparta o grupę adresów i określony czas
* Możliwość filtrowania stron typu https w oparciu o kategorię bez konieczności deszyfrowania całej komunikacji
* Funkcja logowania dostępu do adresów URL. Możliwość określenia osiągniętych zasobów
* Automatyczne generowanie polityk na podstawie analizy ruchu przechodzącego przez firewall
* Funkcjonalność wykrywaniu zdublowanych i nieużywanych polityk
* Możliwość zarządzania urządzeniem przy wykorzystaniu protokołów HTTP i HTTPS, SSH, Telnet oraz z poziomu linii komend
* Możliwość tworzenia kopii zapasowych, eksportowania i przywracania konfiguracji
* Urządzenie musi posiadać wewnętrzny dysk twardy lub kartę Flash o pojemności minimum 64GBG w celu logowania i tworzenia raportów dotyczących np.:
* Analizy ruchu z uwzględnieniem nazwy użytkownika, adresu IP, rodzaju aplikacji, ilości transmitowanych danych
* Statystyki dostępu do stron www z uwzględnieniem kategorii stron www oraz witryn www
* Możliwość tworzenia cyklicznych raportów i wysyłania ich na wskazany adres e-mail

Zamawiający dopuszcza możliwość zaoferowania rozwiązania które funkcje logowania i raportowania wymagane powyżej będzie realizowało za pomocą zewnętrznego systemu. W takim przypadku należy zaoferować rozwiązanie z dedykowanym serwerem sprzętowym wyposażonym w dysk twardy z przestrzenią na logi o powierzchni minimum 64GB oraz wszystkimi niezbędnymi licencjami do prawidłowego działania. W przypadku zaoferowania zewnętrznego systemu raportującego wraz z serwerem Zamawiający wymaga aby wszystkie element (typu sprzęt i oprogramowanie) objęte były identycznym wsparciem serwisowym jak oferowane firewalle.

* Firewalle muszą zostać dostarczone z minimum 2 letnią licencją na funkcjonalności IPS/AV/URL Filtering
* Zamawiający wymaga, aby firewalle posiadały minimum 2 letni serwis gwarancyjny. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia
* Dostarczone rozwiązanie musi być nowe, nie używane w żadnych innych projektach, zakupione w oficjalnym kanale sprzedaży. Zamawiający może podczas etapu dostawy żądać oświadczenia producenta bądź oficjalnego przedstawiciela na rynku Polskim o spełnieniu powyższego punktu.”

**Pytanie 2:**

*Czy w ramach wdrożenia Oferent będzie odpowiedzialny za fizyczny montaż urządzeń typu access-point? Jeżeli tak to prosimy o podanie lokalizacji oraz ilości w danych lokalizacjach oraz na jakiej wysokości mają być instalowane dane access-pointy.*

**Odpowiedź 2:**

Zamawiający zamontuje we własnym zakresie urządzenia typu access-point.

**Pytanie 3:**

*Czy w ramach postępowania należy wykonać odpowiednie okablowanie strukturalne celem doprowadzenia okablowania Ethernet do urządzenia typu access-point? Jeżeli tak, to czy można dostać schematy, rysunki które mogą posłużyć do oszacowania kosztów?*

**Odpowiedź 3:**

Zamawiający posiada wykonane okablowanie strukturalne dla urządzeń typu access-point, jak również wykona wymagane okablowanie co do nowych lokalizacji we własnym zakresie.

**Pytanie 4:**

*Czy w ramach wdrożenia należy wykonać planowanie radiowe przed montażem urządzeń typu access-point celem określenia odpowiedniego miejsca instalacji urządzenia?*

**Odpowiedź 4:**

W ramach postępowania wykonywanie tak zwanego planowania radiowego nie jest wymagane.

**Pytanie 5:**

*Czy w ramach wdrożenia należy wykonać testy pokrycia radiowego po wykonaniu wdrożenia oraz konfiguracji urządzeń?*

**Odpowiedź 5:**

W ramach postępowania zamawiający nie wymaga wykonywania testów pokrycia radiowego.

**Pytanie 6:**

*Czy w ramach postępowania patchordy do połączania access-pointów, switchy, firewalla mają być zapewnione przez wykonawcę? Jeżeli tak to prosimy o podanie ilości, typy kabli oraz długości.*

**Odpowiedź 6:**

W ramach postepowania zamawiający wymaga dostarczenia opisanego w punkcie 4.1.9. - 150 sztuk RJ45-RJ45 kat 6. Należy dostarczyć okablowanie opisane w punkcie 4.1.4 „Z każdym oferowanym kontrolerem należy dostarczyć dwa kable połączeniowe DAC 10G o długości co najmniej 1,5 m. do połączenia każdego kontrolera z dwoma przełącznikami rdzeniowymi.”

Zamawiający informuje jednocześnie, iż zmienia zapisy SIWZ załącznik nr 1.3. „Opis przedmiotu zamówienia dla zadania nr 3”, pkt 1.4 na:

„Dostawa wraz z konfiguracją stacji wyniesionych wraz z instalacją antenową. Zdalne sterowanie radiotelefonem typu DM4600e. Urządzenie umożliwiające sterowanie na odległość poprzez wykorzystanie sieci IP, wszystkie funkcje dostępne z front oryginalnego panelu radiotelefonu. Stacje wyniesione w ilości sztuk 3 pozwalające na obsługę radiostacji wyniesionych za pomocą konsoli posiadanej przez zamawiającego (konsola dyspozytorska TRX). W ramach postępowania należy dostarczyć dwie radiostacje wraz ze sterowaniem po IP oraz 3 sztuki instalacji antenowych. Jeden komplet w celu implementacji radiostacja DM4600e plus sterowanie IP udostępni zamawiający.

Uruchomienie radiostacji wyniesionych w dwóch lokalizacjach:

* Poligon SAPSP w miejscowości Kościelec 133, 32-100 Kościelec (2 radiostacje wraz z instalacjami antenowymi)
* ul. Węgierska 188, 33-300 Nowy Sącz (1 radiostacja wraz instalacją antenową).”

Powyższe zmiany są wiążące dla wszystkich uczestników postępowania. Wykonawca składający ofertę winien powyższe zmiany do SIWZ uwzględnić podczas sporządzania oferty, pod rygorem odrzucenia oferty, jako oferty niezgodnej z treścią SIWZ.

**Zamawiający informuje, iż na podstawie art. 12a Ustawy Prawo zamówień publicznych** **z dnia 29 stycznia 2004 r. (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.) przedłuża termin składania ofert z dnia 30.09.2020 r. do godz. 1200 na dzień 02.10.2020 r. do godz. 1200. Jednocześnie informuje, iż publiczne otwarcie ofert odbędzie się w dniu 02.10.2020 r. o godz. 1200 w siedzibie zamawiającego.**

**Komendant**

**Szkoły Aspirantów Państwowej Straży Pożarnej**

**w Krakowie**

**/-/**

**mł. bryg. mgr inż. Marek CHWAŁA**